2 November 2005

Ms. Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

Re: ***Ex Parte* Communication**
In the Matter of : Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, RM-10865

Dear Ms. Dortch:

This is to inform you that Stephen J. Lukasik and Anthony M. Rutkowski, in their personal professional capacities, provided the attached letter and article concerning the subject proceeding to Chairman Martin, Commissioners Abernathy, Copps and Adelstein, and Daniel Gonzalez, Julius Knapp, Jeffery Goldthorp, Geraldine Matise, and Kenneth Moran.

Pursuant to the Commission's rules, this *ex parte* letter together with the communication are being filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceeding.

Respectfully submitted,

/s/

Anthony M. Rutkowski
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

1 November 2005

Kevin J. Martin, Chairman
Office of the Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington DC 20554

Re: **Appeal of *First Order,*** Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, RM-10865

Dear Chairman Martin:

In light of the recent Appeal of the Commission's CALEA *First Order,* we felt it appropriate as senior professionals and former government officials in the field to speak out in support of FCC efforts to assert its authority to deal more effectively and extensively with communications infrastructure protection, homeland security, and forensic support for law enforcement.

We believe the attached statement entitled "LET THE FCC DO ITS JOB IN PROTECTING THE NATIONAL COMMUNICATIONS INFRASTRUCTURE AND ITS USERS" articulates the basic considerations and a framework for action among concerned professionals, the industry, and government.

Sincerely,

/s/

Stephen J. Lukasik
1714 Stone Canyon Road
Los Angeles, CA 90077
mailto: steve@gnsl.org

/s/
Anthony M. Rutkowski
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

cc: Commissioner Kathleen Q. Abernathy
Commissioner Michael J. Copps
Commissioner Jonathan S. Adelstein
Daniel Gonzalez
Julius Knapp
Jeffery Goldthorp
Geraldine Matise
Kenneth Moran

1 November 2005

LET THE FCC DO ITS JOB IN PROTECTING THE NATIONAL COMMUNICATIONS INFRASTRUCTURE AND ITS USERS

Stephen J. Lukasik and Anthony M. Rutkowski[1]

On October 25, a small group of largely Washington D.C. lobbying organizations went to the U.S. Court of Appeals to challenge a new FCC *CALEA Order* that requires providers of Internet access and VoIP be able to extract digital forensic evidence when required by a court order.[2]

In the past, this kind of challenge by such groups was part of the "fun and games" of the Washington K-Street scene. Today, however, in light of the enormous scaling of network vulnerabilities, attacks, and cybercrime, as well as the events of 9/11, it is difficult to believe that such challenges to responsive, responsible FCC actions would continue. The challenge also stands in stark contrast to other countries where far more extensive forensic requirements have been cooperatively and effectively established and implemented among government authorities and network providers.

The good news is that this latest challenge will almost certainly fail quickly because the FCC *CALEA Order* was very carefully written to comport with the law, with the intent of Congress, and perhaps most importantly, with the needs of the nation for trusted and available public communications infrastructure and services. We describe here why this is important.

ORIGINS AND HISTORY

The entire history of the FCC, going back to its origins in 1934 and all the subsequent grants of authority by Congress, and long affirmed by the Supreme Court, rest on the fundamental understanding that the Commission is uniquely entrusted with making "...available, so far as possible, to all the people of the United States...a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications." These core responsibilities are part of what is commonly known as *Title I authority*.

---

[1] Dr. Lukasik is former Director, Defense Advanced Projects Research Agency; former Chief, FCC Office of Science & Technology; and is currently engaged in a number of counter-terrorism activities related to cybercrime and critical infrastructure protection.
Mr. Rutkowski is currently Vice President for Regulatory Affairs and Standards with VeriSign, active in a broad array of national and international security related forums, and has enjoyed a diverse 40 year career in public and private sectors, including serving as Dr. Lukasik's staff advisor at the FCC, and as Chief of International Telecommunications Regulation at the ITU in Geneva. The views expressed here his own and do not necessarily represent those of VeriSign.

[2] *See First Report and Order and Further Notice of Proposed Rulemaking in the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, September 23, 2005.

More than 18 months ago, the FCC began a comprehensive look at the nation's newly emerging public communications infrastructure being built on open Internet protocols and wireless technologies by a much more diverse set of operators and service providers than has heretofore been the case. The focus was on new regulatory frameworks and capability requirements necessary to perform the Commission's responsibilities in this rapidly emerging Next Generation Network world.

One of the first focus areas dealt with the challenge of protecting both users and the infrastructure itself through the ability of operators to produce digital forensic evidence when required by a court. This need has always existed, but was given special prominence through Congress's 1994 *Communications Assistance to Law Enforcement Act* (CALEA). These additional FCC responsibilities are known as *CALEA authority*. Over the past decade, the mounting network-based economic disruptions and theft, fraud, kidnappings, exploitation of children, identity theft, SPAM, stalking, terrorism, damage to infrastructure, and other assorted cybercrimes became impossible to ignore.

Four cycles of public comments, briefings, and numerous industry outreach efforts ensued over the past two years, including a close examination of global developments. Finally, the Commission last month released its *CALEA Order* proposing the legal foundation on which they would proceed, as well as the scope of its capability requirements.

The Commission's approach was very deliberate and conservative - carefully and narrowly written to reflect exactly what Congress intended, as well as what was appropriate to meet its Title I responsibilities. The *Order* also reflected the findings of the Supreme Court at the end of the last term in the landmark *Brand-X Decision* that underscored the importance of the Commission's unique expertise and responsibility for the national public communications infrastructure today.

SOLID FOUNDATIONS AND PRECISE SCOPE

The Commission exhaustively examined both its longstanding responsibility and authority to protect the national communications infrastructure and its users, as well as the specific language of CALEA. Congress in 1994 repeatedly emphasized that CALEA was a generic requirement to assist law enforcement in obtaining needed forensic evidence that should evolve with the technology and its deployment as public services. The capability requirements applied to "services or facilities that enable the subscriber to make, receive or direct calls." The FCC, in consultation with law enforcement and public proceedings, was also to serve as the final arbiter as to what was required as infrastructure evolution occurred.

A key provision placed in the Act was explicit authority to apply the requirements to any "...person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is

in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of [CALEA]."

The FCC pragmatically decided that there were two critical places in the national communications infrastructure where digital forensic evidence existed - in the facilities of 1) broadband Internet access providers and 2) voice telephone service providers to the extent they were interconnected with the public telephone infrastructure. These represented minimal technological choke points where forensic evidence was uniquely available - not only for evidentiary purposes, but also for network management and the protection of networks. It is worth noting that other regulatory bodies throughout the world have come to similar conclusions.

Indeed, the global nature of these requirements led the FCC to note that the forensic capabilities were already being implemented in infrastructure systems at low cost with no adverse impact on performance or evolution of the technology. These considerations were factors that Congress asked the FCC to evaluate in exercising its authority.

The FCC in its *Order* took the right steps under its CALEA authority. The reality is that the Commission could also require the same capabilities entirely under its Title I authority and responsibilities, if not other longstanding authority provided by Congress.

In fact, proceeding to exercise Title I authority has become increasingly important as the Commission moves away from common carrier regulatory models, and puts into place needed public infrastructure capability requirements for open Next Generation Networks. This includes everything from public safety and emergency preparedness requirements to consumer protection to competitive unbundling and Universal Service Fund reform.

NEEDED NEXT STEPS FOR CRITICAL INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

National infrastructures have a lot in common with, and indeed they all represent, "public commons." "Roadway" is a useful metaphor. When you use public infrastructures you can not be anonymous because each user interacts with other users and with the system operator: thus we have license plates on cars (plus other information-providing stickers), EZ pass ID for added convenience, operator license attesting to technical qualifications, vehicle VIN, bills of sale and titles, records of transgressions, DOT labeling on trucks, identification of hazardous cargo, etc. So too with providers and users of public networks.

Perhaps most importantly, public infrastructures are "generally available to the public," and have important characteristics and user expectations such as substantial availability (especially during and after emergencies), and for the protection of users. These are the FCC's most important Title I responsibilities, and are shared today with the President, the Department of Homeland Security, and the Department of Justice. Providers and users of these public infrastructure services in exchange for ubiquitous access to national and

global networks, undertake obligations and responsibilities established in law, regulations, and technical standards.

The events of the past several years - including natural disasters still in progress - have underscored the importance of the FCC's Title I authority, and compel a much more active role in understanding the vulnerabilities and demonstrating leadership in bringing about corrective actions. Chairman Martin's recent establishment of a Homeland Security Bureau to achieve these aims within the FCC is a reflection of these increasingly demanding circumstances.

CALEA requirements and their production of critical digital forensic evidence is an example of one set of needs. Other related and even more important capabilities involve the ability to identify and authenticate providers and users of the public infrastructure, including the numbers and addresses they use. Such interoperable trusted directory capabilities, that are receiving worldwide attention, go to the heart of a stable and viable public infrastructure.

Much more extensive collaboration in these areas is also needed not only among U.S. government agencies, but also with counterparts throughout the world through established intergovernmental collaborative mechanisms such as the ITU and the Cybercrime Convention. The network infrastructure is global, and when it starts failing by accident or attack, necessary international detection and rapid emergency response capabilities will be critical to any kind of meaningful response and followup preventative actions.

This need is underscored by a parallel technical development in virtually all infrastructures such as those that meet transportation, energy, water, and other critical societal needs. This is that the communication network is becoming an integral part of the internal operations of all of them, and thus attacks on the network have implications reaching far beyond communication.

What is sorely needed at this point is for the K-Street community to lobby on behalf of the nation, the industry, and the users to protect and strengthen the national communications infrastructure against malicious, criminal, and irresponsible users. Running off to Appellate Court after every FCC infrastructure protection Order is in the long-term interests of no one.

* * *